UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY
NEWARK DIVISION

DESTINY PALMITER, on behalf of herself and all others similarly situated, Plaintiff, v. HEALTHEC LLC, Defendant.	Case No. 24-cv-27 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Destiny Palmiter, on behalf of herself and all others similarly situated, states as follows for her class action complaint against Defendant, HealthEC LLC, ("HealthEC" or "Defendant"):

INTRODUCTION

1. Between July 14, 2023, and July 23, 2023, HealthEC, a population health technology company that provides services to other entities, lost control over its computer network and the highly private information stored on the computer network in a data breach perpetrated by cybercriminals ("Data Breach"). On information and belief, the Data Breach's impact has been substantial, affecting at least 1 million consumers.

2. HealthEC's breach differs from typical data breaches because it affects consumers who had no relationship with HealthEC, never sought one, and never consented to HealthEC's collecting and storing their information.

3. On information and belief Data Breach began on or around July 14, 2023, and was

allowed by Defendant to continue until July 23,2023, providing cybercriminals unfettered access to consumers' highly private information for at least nine days.

4. Following an internal investigation, Defendant learned cybercriminals gained unauthorized access to consumers' personally identifiable information ("PII") and private health information ("PHI") (collectively with PII, "Sensitive Information").

5. On information and belief, cybercriminals bypassed Defendant's inadequate security systems to access consumers' Sensitive Information in its computer systems.

6. On or about December 22, 2023, HealthEC finally notified State Attorneys General and many Class Members about the widespread Data Breach ("Breach Notice"). Plaintiff's Data Breach Notice is attached as **Exhibit A**.

7. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its victims how many people were impacted, when Defendant actually discovered the breach, how the breach happened, or why it took the Defendant five months after discovering the Breach to begin notifying victims that hackers had gained access to highly private Sensitive Information.

8. Defendant's failure to timely detect and report the Data Breach made its victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of Sensitive Information misuse.

10. In failing to adequately protect consumers' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and

harmed an unknown number of its consumers.

11. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their Sensitive Information. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiff, Destiny Palmiter, is a Data Breach victim.

13. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

14. Plaintiff, Destiny Palmiter, is a natural person and citizen of Michigan, residing in Lincoln Park, Michigan where she intends to remain. Ms. Palmiter is a Data Breach victim, receiving HealthEC's Breach Notice on December 22, 2023.

15. Defendant, HealthEC, is a New Jersey and Delaware corporation with its principal place of business at 343 Thornall Suite # 630, Edison, NJ 08837.

JURISDICTION & VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; there are more than 100 members in the proposed class; Plaintiff and Defendant are citizens of different states.

17. HealthEC is incorporated in Delaware and maintains its principal place of business in 343 Thornall Suite # 630, Edison, NJ 08837. HealthEC is thus a Delaware and New Jersey

citizen.

18. This Court has personal jurisdiction over HealthEC because it is a citizen in this District and maintains its headquarters and principal place of business in this District.

19. Venue is proper because HealthEC maintains its headquarters and principal place of business in this District.

BACKGROUND FACTS

HealthEC

20. According to its website, HealthEC boasts itself as the "most modern, AI-enabled population health management platform" that "enable[s] value-based health systems and care organizations to identify high-risk patients, close care gaps and recognize barriers to optimal care."[1] HealthEC boasts $30 million in annual revenue. [2]

21. HealthEC's services are specialized for healthcare providers who oversee highly sensitive data. HealthEC thus must oversee, manage, and protect the Sensitive Information of its clients' patients.

22. On information and belief, these third-party consumers, whose Sensitive Information was collected by HealthEC, do not do any business with HealthEC.

23. After collecting its consumers' Sensitive Information, HealthEC maintains the Sensitive Information in its computer systems.

24. In working with third party consumers' highly sensitive data, HealthEC advertises in its privacy policy that it "is committed to protecting the privacy of the personally identifiable information that we collect from you."[3]

---

[1] HealthEC, https://www.healthec.com/ (last visited January 3, 2024).
[2] HealthEC, Zippia, https://www.zippia.com/healthec-careers-1401116/revenue/ (last visited January 3, 2024).
[3] Privacy Policy, HealthEC, https://mneconnect.healthec.com/ProdMNeConnectAdmin/Privacy_Policy.aspx (last visited January 3, 2024).

25. It further assures consumers that "HealthEC has implemented generally accepted standards of technology and operational security in order to protect Personal Info from loss, misuse, alteration, or destruction. Only authorized HealthEC personnel are provided access to Personal Info, and these employees are required to treat this information as confidential."[4]

26. As a self-proclaimed leader in its field that regularly handles highly sensitive aspects of its clients' business, HealthEC understood the need to protect its client's consumers data and prioritize its data security.

27. Despite recognizing its duty to do so, on information and belief, HealthEC has not implemented reasonably cybersecurity safeguards or policies to protect its consumers' Sensitive Information or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, HealthEC leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' Sensitive Information.

HealthEC Fails to Safeguard Consumers' Sensitive Information

28. Plaintiff is unsure how HealthEC got her information but assumes her prior healthcare provider, Beaumont ACO, provided HealthEC with her Sensitive Information, including but not limited to her name, date of birth, medical information, as well as billing and claims information.

29. On information and belief, HealthEC collects and maintains consumers' Sensitive Information in its computer systems.

30. In collecting and maintaining Sensitive Information, HealthEC implicitly agrees it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

[4] *Id*.

31. According to the Breach Notice, HealthEC "became aware of suspicious activity potentially involving our network[.]" HealthEC admits that, following an internal investigation, it discovered its "systems were accessed by an unknown actor between July 14, 2023 and July 24, 2023, and during this time certain files were copied." Ex. A.

32. In other words, Defendant's investigation revealed that its network had been hacked by cybercriminals and that Defendant's inadequate cyber and data security systems and measures allowed those responsible for the cyberattack to obtain files containing a treasure trove of thousands of HealthEC's consumers' personal and highly private Sensitive Information.

33. Additionally, Defendants admitted that Sensitive Information was actually stolen during the Data Breach confessing that the information was not just accessed, but "**copied**" from its system. (Emphasis added) Ex. A.

34. Due to its intentionally obfuscating nature, it is unclear when HealthEC actually discovered the Data Breach.

35. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's Sensitive Information for theft and sale on the dark web.

36. In response to the Data Breach, HealthEC contends that it has or will be taking "steps to reviewing our existing policies and procedures." Ex. A. Although HealthEC fails to expand on how these alleged "reviews" would prevent a future breach, these reviews of policies and procedures should have been conducted before the Data Breach.

37. Through its Breach Notice, HealthEC recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of identity theft and fraud, by reviewing account statements, explanation of benefits statements, and monitoring free credit reports for suspicious activity and to detect errors."

Ex. A.

38. HealthEC further recognized through its Breach Notice, its duty to implement reasonable cybersecurity safeguards or policies to protect its consumers' Sensitive Information, promising that, despite the Data Breach demonstrating otherwise, it has an "ongoing commitment to your privacy and security of information in our care [.]" Ex. A.

39. On information and belief, HealthEC has offered several months of complimentary credit monitoring services to victims during that time, which does not adequately address the lifelong harm that victims will face following the Data Breach.

40. Even with only several months of credit monitoring, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

42. On information and belief, HealthEC failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

43. Defendant's data security obligations were particularly important given the

substantial increase in cyberattacks and/or data breaches in the healthcare and healthcare adjacent industry preceding the date of the breach.

44. In light of recent high profile data breaches at other healthcare partner and provider companies, HealthEC knew or should have known that their electronic records and consumers' Sensitive Information would be targeted by cybercriminals.

45. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[5] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[6]

46. Indeed, cyberattacks against healthcare and healthcare adjacent industries have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [7]

47. Cyberattacks on medical systems and healthcare partner and provider companies like Defendant's have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often

[5] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited May 9, 2023).
[6] *Id.*
[7] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited May 9, 2023).

have lesser IT defenses and a high incentive to regain access to their data quickly."[8]

48. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including HealthEC.

Plaintiff's Experience and Injuries

49. Ms. Palmiter received HealthEC's breach notice on or about December 22, 2023. She is unsure why Defendant is in possession of her Sensitive Information but assumes her previous healthcare provider, Beaumont ACO, provided HealthEC with her personal information.

50. Regardless, HealthEC has a duty to safeguard her information according to its internal policies and state and federal law.

51. HealthEC deprived Ms. Palmiter of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for five months.

52. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

53. Plaintiff does not recall ever learning that her Sensitive Information was compromised in a data breach incident, other than the breach at issue in this case.

54. As a result of the Data Breach and the recommendation of Defendant's Notice Ms. Palmiter has spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

55. Ms. Palmiter has and will spend considerable time and effort monitoring her

[8] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited May 9, 2023).

accounts to protect herself from identity theft. Ms. Palmiter fears for her personal financial security and uncertainty over what Sensitive Information exposed in the Data Breach. Ms. Palmiter has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

56. Plaintiff suffered actual injury from the exposure of her Sensitive Information — which violates her rights to privacy.

57. Ms. Palmiter has suffered actual injury in the form of damages to and diminution in the value of her Sensitive Information —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

58. Ms. Palmiter has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

59. Ms. Palmiter has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

60. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

61. The ramifications of Defendant's failure to keep Plaintiff's and the Class's Sensitive Information secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, date of birth, Social Security number, or driver's license number, without permission, to commit fraud or other crimes.

62. The types of Sensitive Information compromised and potentially stolen in the Data Breach is highly valuable to identity thieves. The consumers' stolen Sensitive Information can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

63. Identity thieves can also use the stolen data to harm Plaintiff and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health- related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

64. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of the Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in their possession.

65. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

66. The value of Plaintiff's and the proposed Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

67. It can take victims years to spot identity or Sensitive Information theft, giving

criminals plenty of time to use that information for cash.

68. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

69. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

70. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

71. Defendant disclosed the Sensitive Information of Plaintiff and the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

72. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, as evidenced by its complete failure to prevent malware in its systems, demonstrates a willful and conscious disregard for privacy, and has exposed Sensitive Information of Plaintiff and members of the proposed Class to unscrupulous operators, con-artists, and criminals.

73. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

74. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

75. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of private information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

76. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

77. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

78. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

79. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Violated HIPAA

80. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients, or in this case, consumers' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of

protected health information.[9]

81. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Sensitive Information is properly maintained.[10]

82. The Data Breach itself resulted from a combination of inadequacies showing Defendant's failure to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those

[9] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[10] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

83. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant Fails to Comply with Industry Standards

84. As noted above, experts studying cyber security routinely identify entities in possession of Sensitive Information as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

85. Several best practices have been identified that a minimum should be implemented by companies in possession of Sensitive Information, like Defendant, including but not limited to:

educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

86. Other best cybersecurity practices that are standard for companies like Defendant include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

87. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

88. These foregoing frameworks are existing and applicable industry standards for a company's obligations to provide adequate data security for its consumers. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

89. Plaintiff brings this action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the

Federal Rules of Civil Procedure.

90. Plaintiff sues on behalf of herself and the proposed Class ("Class"), defined as follows:

> **All individuals in the United States whose Sensitive Information was accessed without authorization in the Data Breach, including all those who received a notice of the Data Breach.**

91. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

92. Plaintiff reserves the right to amend the class definition.

93. This action satisfies the numerosity, commonality, typicality, and adequacy requirements for suing as representative parties:

94. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of at least 1 million members, far too many to join in a single action;

95. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

96. **Typicality.** Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

97. **Adequacy.** Plaintiff will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with Class members' interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

98. **Commonality.** Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

a. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant was negligent in maintaining, protecting, and securing Sensitive Information;

d. Whether Defendant breached contract promises to safeguard Plaintiff and the Class's Sensitive Information;

e. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. Whether Defendant's Breach Notice was reasonable;

g. Whether the Data Breach caused Plaintiff's and the Class' injuries;

h. What the proper damages measure is; and

i. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

99. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

100. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

101. Plaintiff and members of the Class entrusted their Sensitive Information to HealthEC. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their Sensitive Information and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the Sensitive Information of Plaintiff and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

102. HealthEC was under a basic duty to act with reasonable care when it undertook to collect, create, and store Plaintiff's and the Class's Sensitive Information on its computer system, fully aware–as any reasonable entity of its size would be–of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

103. Defendant knew that the Sensitive Information of Plaintiff and the Class was information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the Sensitive Information of Plaintiff and the Class was wrongfully disclosed.

104. By being entrusted by Plaintiff and the Class to safeguard their Sensitive Information, Defendant had a special relationship with Plaintiff and the Class. Plaintiff's and the Class's Sensitive Information was provided to HealthEC with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

105. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' Sensitive Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite failures and intrusions, and allowing unauthorized access to Plaintiff's and the Class's Sensitive Information.

106. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their Sensitive Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the Sensitive Information of Plaintiff and the Class and all resulting damages.

107. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' Sensitive Information.

108. As a result of Defendant's failure, the Sensitive Information of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Sensitive Information was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their Sensitive Information in that it is now easily available to hackers on the Dark Web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

109. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

110. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Sensitive Information.

111. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customer information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's Sensitive Information.

112. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

113. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its consumers, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

114. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the

healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

115. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Sensitive Information.

116. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

117. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

118. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed supra. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

119. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff

and members of the Class, Plaintiff and members of the Class would not have been injured.

120. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

121. Had Plaintiff and the Class known that Defendant did not adequately protect their Sensitive Information, Plaintiff and members of the Class would not have entrusted Defendant with their Sensitive Information.

122. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

123. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Sensitive Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

124. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as HealthEC fails to undertake appropriate and adequate measures to protect their Sensitive Information in its continued possession.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

125. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

126. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly confidential Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

127. Defendant owed a duty to its consumers, including Plaintiff and the Class, to keep this information confidential.

128. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class members' Sensitive Information is highly offensive to a reasonable person.

129. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

130. The Data Breach constitutes an intentional interference with Plaintiff and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

131. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

132. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation

efforts.

133. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

134. As a proximate result of Defendant's acts and omissions, the Sensitive Information of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

135. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Sensitive Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

136. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Sensitive Information of Plaintiff and the Class.

137. In addition to injunctive relief, Plaintiff, on behalf of herself and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT IV
Breach of Contract
(On Behalf of Plaintiff and the Class)

138. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

139. HealthEC entered into various contracts with its healthcare provider clients to

provide its services to its clients.

140. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential medical information that HealthEC agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Sensitive Information belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

141. HealthEC knew that if it were to breach these contracts with its clients, the clients' consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their Sensitive Information.

142. HealthEC breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' Sensitive Information.

143. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by HealthEC's failure to use reasonable data security measures to store their Sensitive Information, including but not limited to, the actual harm through the loss of their Sensitive Information to cybercriminals.

144. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

145. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

146. This claim is pleaded in the alternative to the breach of contract claim.

147. Plaintiff and Class Members conferred a monetary benefit on Defendant when

Defendant's clients provided Plaintiff's and Class Members' Sensitive Information to Defendant, which Defendant collected.

148. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Sensitive Information.

149. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

150. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

151. Defendant acquired the monetary benefit and Sensitive Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

152. If Plaintiff and Class Members knew that Defendant had not secured Sensitive Information, they would not have agreed to have their Sensitive Information provided to Defendant.

153. Plaintiff and Class Members have no adequate remedy at law.

154. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) the loss of the opportunity how their Sensitive Information is used; (ii) the compromise, publication, and/or theft

of their Sensitive Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Sensitive Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in their continued possession and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

155. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

156. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT VI
New Jersey Consumer Fraud Act
N.J.S.A. § 56:8-1, *et seq.*
(On Behalf of Plaintiff and the Class)

157. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

158. The New Jersey Consumer Fraud Act (the "NJCFA"), N.J.S.A. § 56:8-1, *et seq.*, prohibits the act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression or omission, in connection with the sale or advertisement of any merchandise. The

NJCFA applies whether or not any person has in fact been misled, deceived or damaged thereby. N.J.S.A. § 56:8-2.

159. Plaintiff, Defendant, and Class Members are "persons" within the meaning of N.J.S.A. § 56:8-1(d).

160. Defendant sells "merchandise," as defined by N.J.S.A. § 56:8-1, by offering population health technology services to the public.

161. Defendant, operating in New Jersey, engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of population health technology services in violation of N.J.S.A. § 56:8-2, including but not limited to the following:

a. Misrepresenting material facts, pertaining to the sale of population health technology services, to its clients' consumers, including the Plaintiff and Class Members, by representing that they would maintain adequate data security practices and procedures to safeguard Plaintiff's and Class Members' Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts, pertaining to the sale of population health technology services, to its clients' consumers, including the Plaintiff and Class Members, by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class Members' Sensitive Information;

c. Knowingly omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' Sensitive Information with the intent that Plaintiff and Class Members

rely on the omission, suppression, and concealment;

d. Engaging in unconscionable and deceptive acts and practices with respect to the sale of population health technology services by failing to maintain the privacy and security of Plaintiff's and Class Members' Sensitive Information in violation of duties imposed by and public policies reflected in the FTC Act;

e. Engaging in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiff and Class Members in a timely and accurate manner in violation of N.J.S.A. § 56:8-163;

f. Representing on its website that it "is committed to protecting the privacy of the personally identifiable information that we collect from you," when, in fact, HealthEC never implemented the security safeguards needed.

162. The above unlawful and deceptive acts and practices by Defendant was immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

163. Defendant knew or should have known that their data security practices were inadequate to safeguard Plaintiff's and Class Members' Sensitive Information and that the risk of a data breach was highly likely. Defendant's actions in engaging in the above-listed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

164. Plaintiff and Class Members reasonably expected that Defendant would protect their Sensitive Information and reasonably expected that Defendant would provide truthful statements on their website and privacy policies, and that it would be safe to provide HealthEC

with their information. These representations and affirmations of fact made by Defendant, and the facts they concealed or failed to disclose, are material facts that were likely to deceive reasonable consumers, and that reasonable consumers would, and did, rely upon in deciding whether or not to entrust their information to HealthEC. Defendant, moreover, intended for consumers, including Plaintiff and Class Members, to rely on these material facts.

165. As a direct and proximate result of Defendant's unconscionable and deceptive acts and practices, Plaintiff and Class Members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Sensitive Information.

166. Plaintiff and Class Members seek relief under N.J.S.A. § 56:8-19, including but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demand that this matter be tried before a jury.

Dated: January 3, 2024

Respectfully submitted,

By: */s/ Patrick Howard*

Patrick Howard (NJ Atty ID #02280-2001)
SALTZ MONGELUZZI & BENDESKY, P.C.
8000 Sagemore Drive, Suite 8303
Marlton, NJ 08053
Tel: (856) 751-0868
phoward@smbb.com

TURKE & STRAUSS LLP
Samuel J. Strauss (*pro hac vice admission forthcoming*)
Raina Borrelli (*pro hac vice admission forthcoming*)
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Daniel Srourian, Esq.* (*pro hac vice admission forthcoming*)
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd. Suite 1710
Los Angeles, California 90010
Telephone: (213) 474-3800
Facsimile: (213) 471-4160
Email: daniel@slfla.com

Attorneys for Plaintiff and Proposed Class